

ABSTRAK

Komunikasi grup dalam jaringan terdistribusi memerlukan mekanisme manajemen kunci yang kuat untuk menjamin kerahasiaan data antaranggota. Dinamika anggota yang tinggi mengharuskan adanya pembaruan kunci (*rekeying*) secara berkala demi mempertahankan *forward secrecy* dan *backward secrecy*. *Tree-Based Group Diffie-Hellman* (TGDH) merupakan protokol manajemen kunci kelompok yang memanfaatkan struktur pohon biner untuk meningkatkan efisiensi *rekeying*. Penelitian ini memfokuskan analisis pada algoritma *Rebuild* dalam TGDH, yang berfungsi menyusun ulang struktur pohon secara periodik guna menjaga keseimbangan pohon. Evaluasi performa dilakukan melalui simulasi jaringan terdistribusi dengan mengukur biaya komputasi berdasarkan jumlah eksponensiasi dan biaya komunikasi berdasarkan jumlah simpul yang diperbarui (*renewed nodes*). Hasil penelitian ini diharapkan dapat memberikan gambaran komprehensif mengenai efisiensi algoritma *Rebuild* dalam mendukung keamanan di komunikasi grup yang dinamis.

Kata kunci : TGDH, *rekeying*, *Rebuild*, *group key management*, komunikasi grup

ABSTRACT

Group communication in distributed networks requires a robust key management mechanism to ensure data confidentiality among members. High member turnover necessitates periodic key updates (rekeying) to maintain forward secrecy and backward secrecy. Tree-Based Group Diffie-Hellman (TGDH) is a group key management protocol that utilizes a binary tree structure to improve rekeying efficiency. This study focuses its analysis on the Rebuild algorithm in TGDH, which serves periodically reorganize the tree structure to maintain tree balance. Performance evaluation was conducted through distributed network simulations by measuring computational cost based on the number of exponentiations and communication cost based on the number of renewed nodes. The results of this study are expected to provide comprehensive overview of the efficiency of the Rebuild algorithm in supporting security in dynamic group communications.

Keywords : TGDH, rekeying, Rebuild, group key management, group communication

